Cisco Catalyst SD-WAN ソフトウェアのセキュリティ強化リリース：2026 年 8 月

アドバイザリーID : cisco-sa-hardening-sdwan-faLcR3K
初公開日 : 2026-08-05 16:00
バージョン 1.0 : Final
CVSSスコア : 9.9
回避策 : No workarounds available
Cisco バグ ID :

CVE-2026-20303
CVE-2026-20304
CVE-2026-20312
CVE-2026-20313
CVE-2026-20310

日本語による情報は、英語による原文の非公式な翻訳であり、英語原文との間で内容の齟齬がある場合には、英語原文が優先します。

概要

予防的なセキュリティと製品の品質に対するシスコの継続的な取り組みの一環として、Cisco Catalyst SD-WANソフトウェアエンジニアリングチームは、包括的な社内セキュリティレビューを実施しました。このレビューの結果、内部で発見された複数の脆弱性に対処するソフトウェア強化リリースが開発されました。

これらの脆弱性は内部テストで発見されたものであり、現時点でエクスプロイトの事例は確認されていません。パッチの適用と開示プロセスの合理化を支援するために、シスコでは、これらの問題を基盤となる脆弱性クラス(Common Weakness Enumeration(CWE))別にグループ化し、各CWEグループにCommon Vulnerabilities and Exposures ID(CVE ID)を1つ割り当てています。

シスコはこれらの脆弱性に対処するソフトウェアアップデートをリリースしています。これらの脆弱性に対処する回避策はありません。

このアドバイザリは、次のリンクより確認できます。
https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K

該当製品

脆弱性のある製品

これらの脆弱性は、デバイスの設定に関係なく、Cisco Catalyst SD-WANソフトウェアに影響を与えます。

これらの脆弱性は、以下を含むすべての展開タイプに影響します。

- オンプレミス展開
- Cisco SD-WAN Cloud-Pro
- Cisco SD-WAN Cloud（Cisco Managed）
- 政府/自治体向け Cisco SD-WAN（FedRAMP）

脆弱性が存在する Cisco ソフトウェアリリースについては、このアドバイザリの「修正済みソフトウェア」セクションを参照してください。

脆弱性を含んでいないことが確認された製品

このアドバイザリの「脆弱性のある製品」セクションに記載されている製品のみが、これらの脆弱性の影響を受けることが分かっています。

詳細

次の表に、これらのソフトウェア強化リリースで対処されている脆弱性クラスの概要を示します。各 CVE ID に割り当てられる CVSS スコアは、その特定の CWE カテゴリ内で最も影響の大きい 1 つの根本的な脆弱性がもたらす可能性がある最大のシビラティ（重大度）を表しています。

CVE ID	CVSS最高スコア	脆弱性クラス（最高レベルのCWE）	説明
CVE-2026-20303	9.9	CWE-20	不適切な入力検証（入力検証、パストラバーサル、外部パス制御など）
CVE-2026-20304	9.9	CWE-284	不適切なアクセス制御（承認、認証、権限、およびバイパスなど）
CVE-2026-20310	9.9	CWE-59	ファイルアクセス前の不適切なリンク解決
CVE-2026-20312	8.8	CWE-312	機密情報のクリアテキストでの保存
CVE-2026-20313	7.7	CWE-1284	入力で指定された数量の検証が不適切

回避策

これらの脆弱性に対処する回避策はありません。

修正済みソフトウェア

この脆弱性を完全に修正し、本アドバイザリに記載されているような将来のリスクを回避するた

めに、シスコでは、本アドバイザリに記載されている修正済みソフトウェアにアップグレードすることを強く推奨します。

修正済みリリース

次の表では、左の列にシスコ ソフトウェアリリースを記載しています。右の列は、リリースがこのアドバイザリに記載されている脆弱性の影響を受けるかどうか、およびこれらの脆弱性に対する修正を含む最初のリリースを示しています。このセクションの表に記載されている適切な修正済みソフトウェアリリースにアップグレードすることをお勧めします。

Cisco Catalyst SD-WAN リリース	First Fixed Release（修正された最初のリリース）
20.91 より前	修正済みリリースに移行。
20.9	20.9.10
20.10	20.12.8.1
20.111	20.12.8.1
20.12	20.12.8.1
20.131	20.15.6
20.141	20.15.6
20.15	20.15.6
20.161	20.18.4
20.18	20.18.4
26.1	26.1.2

1. これらのリリースは、 ソフトウェアメンテナンスが終了しています。シスコでは、サポートされているリリースにアップグレードすることを強く推奨します。

シスコの Product Security Incident Response Team（PSIRT; プロダクト セキュリティ インシデント レスポンス チーム）は、このアドバイザリに記載されている該当するリリース情報と修正済みリリース情報のみを検証します。

シスコは、クラウドベースの Cisco SD-WAN Cloud（Cisco Managed）リリース 20.15.602 においても、これらの脆弱性に対処しています。ユーザの対処は必要ありません。サービス GUI のヘルプ機能を使用すると、現在の修復ステータスやソフトウェアバージョンを確認できます。

その他の情報が必要な場合は、Cisco Technical Assistance Center（TAC）もしくは契約しているメンテナンスプロバイダーにお問い合わせください。

不正利用事例と公式発表

Cisco PSIRT では、本アドバイザリに記載されている脆弱性の不正利用事例とその公表は確認しておりません。

出典

これらの脆弱性は、既存のテストプロセスおよびフロンティアの AI モデルを使用した内部セキュリティテストで発見されました。

URL

https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hardening-sdwan-faLcR3K

改訂履歴

バージョン	説明	セクション	ステータス	日付
1.0	初回公開リリース	—	Final	2026 年 8 月 5 日

利用規約

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。